Cristina Perez Hesano (#027023)
cperez@perezlawgroup.com
PEREZ LAW GROUP, PLLC
7508 N. 59th Avenue
Glendale, AZ 85301
Telephone: (602) 730-7100
Facsimile: (623) 235-6173

CARL V. MALMSTROM
(*pro hac vice forthcoming*)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. JACKSON BLVD., SUITE 1700
CHICAGO, IL 60604
Telephone: (312) 984-0000
Facsimile: (212) 686-0114
malmstrom@whafh.com

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Brian Eitemiller, individually and on behalf of all others similarly situated, Plaintiff, v. On Q Financial, LLC Defendant.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

I. INTRODUCTION

1. Plaintiff Brian Eitemiller ("Plaintiff") brings this class action in this Court against Defendant On Q Financial LLC ("On Q" or "Defendant") for its failure to prevent a cyberattack that resulted in the theft and dissemination (the "Data Breach") of Plaintiff's and other similarly situated consumers' sensitive information, including, upon

information and belief, at least their full names and Social Security numbers ("Personally identifiable information" or "PII").[1, 2]

2. Beginning on February 21, 2024 cyberattackers gained access to Defendant's network through software that Defendant uses for remote access to computers in its network.

3. Defendants reported that, at minimum, this PII included at least names and Social Security numbers.

4. Plaintiff and Class members now face a present and imminent lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

5. The information stolen in cyber-attacks allows the modern thief to assume victims' identities when carrying out criminal acts such as:

- Filing fraudulent tax returns;
- Using your credit history;
- Making financial transactions on behalf of victims, including opening credit accounts in victims' names;
- Stealing benefits that belong to victims; and
- Committing illegal acts which, in turn, incriminate victims.

6. Plaintiff's and Class members' SPI was compromised due to Defendant's

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] *See* https://www.hipaajournal.com/pja-data-breach/, last accessed November 21, 2023.

negligent and/or careless acts and omissions and the failure to protect the SPI of Plaintiff and Class members.

7. As of this writing, there exist many class members who have no idea their SPI has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

8. Plaintiff brings this action on behalf of all persons whose SPI was compromised as a result of Defendant's failure to: (i) adequately protect consumers' SPI, (ii) adequately warn its current and former customers and potential customers of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the "Class"). Defendant's conduct amounts to negligence and violates state statutes.

9. Plaintiff and similarly situated individuals have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished inherent value of SPI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under state consumer protection and data breach notification acts; and (v) the continued and certainly an increased risk to their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI.

II. PARTIES

10. Plaintiff Brian Eitemiller is, and at all times relevant, has been a citizen of Prescott Valley, Arizona.

11. Defendant is an Arizona corporation with its principal place of business located at 3800 N. Central Ave Ste 460, Phoenix, Arizona, 85012.

III. JURISDICTION AND VENUE

12. The Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class member is a citizen of a state different from Defendant.

13. This Court has jurisdiction over Defendant because it operates in this District.

14. Venue is proper in this District under 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendant has harmed Class members residing in this District.

IV. FACTUAL ALLEGATIONS

15. Defendant is a mortgage servicer who handles processing mortgage payments for certain companies that purchase mortgages.

16. As a necessary part of its regular business activities, Defendant collected and stored the PII of Plaintiff and Class members when it obtained those mortgages from

the previous sellers.

17. On information and belief, at no point did Plaintiff or the Class directly provide their PII to Defendant.

18. On or about March 29, 2024, Defendant announced publicly that on or around March 14, 2024, it has discovered "some suspicious activity through the Screen Connect application. On Q Financial engaged a computer forensics investigation firm to conduct an independent investigation into what happened and determine whether personal information may have been accessed or acquired without authorization."[3]

19. Plaintiffs' and class members' PII was in the hands of hackers for over a month before Defendant began notifying them of the Data Breach.

20. Defendant has been distressingly vague on its response to the Data Breach, stating only that "we immediately patched and upgraded the application and began an investigation."[4]

21. As of this writing, Defendants have offered no concrete information on the steps they have taken or specific efforts made to reasonably ensure that such a breach cannot or will not occur again.

22. Defendants are offering minimal additional assistance to Plaintiffs and class members beyond an inadequate 12 months of credit monitoring.

23. This response is entirely inadequate to Plaintiffs and class members who now

[3] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/bfabbdc9-6593-4e0f-a9b5-bf21a94b2329.shtml, last accessed May 8, 2024.
[4] *Id.*

potentially face several years of heightened risk from the theft of their PII and who may have already incurred substantial out-of-pocket costs in responding to the Data Breach.

24. In its Privacy Policy, On Q states:

DISCLOSURE OF YOUR INFORMATION

We may disclose aggregated information about our users, and information that does not identify any individual, without restriction.

We may disclose personal information that we collect or you provide as described in this privacy policy:

- To our subsidiaries and affiliates;
- To contractors, service providers, and other third parties we use to support our business;
- To a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of the Company's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by the Company about our Website users is among the assets transferred;
- To third parties to market their products or services to you if you have not opted out of these disclosures. For more information, see Choices About How We Use and Disclose Your Information;
- To fulfill the purpose for which you provide it;
- For any other purpose disclosed by us when you provide the information; and/or
- With your consent.

We may also disclose your personal information:

- To comply with any court order, law, or legal process, including to respond to any government or regulatory request;
- To enforce or apply our Terms of Use https://onqfinancial.com/terms-of-use and other agreements, including for billing and collection purposes; and/or
- If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of our Company, our customers, or others. This includes exchanging information with other companies and organizations for the purposes of

fraud protection and credit risk reduction.[5]

25. At no point does On Q disclose that it may give PII to hackers or other threat actors.

26. Needless to say, the release of Plaintiff's and Class members' PII was done without their consent and in ways not consistent with Defendant's Privacy Policy.

27. Plaintiff and Class members provided their PII to Defendant (where provided voluntarily) with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

28. Plaintiff and the Class members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class members value the confidentiality of their PII and demand security to safeguard their PII.

29. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PII safe and confidential.

30. Defendant had obligations created by the FTC Act, contract, industry standards, and representations made to Plaintiff and Class members, to keep their PII

[5] https://onqfinancial.com/privacy-policy/, last accessed May 8, 2024.

confidential and to protect it from unauthorized access and disclosure.

31. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII from disclosure.

33. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the medical services industry preceding the date of the breach.

34. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

35. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and

patience to resolve.[6] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[7]

36. The PII of Plaintiff and members of the Class was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the SPI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

37. Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and members of the Class, including Social Security numbers, dates of birth, and other sensitive information, as well as of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and members of the Class a result of a breach.

38. Plaintiff and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

---

[6] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf, last accessed May 8, 2024.

[7] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

39. The injuries to Plaintiff and members of the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the SPI of Plaintiff and members of the Class.

40. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

41. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

42. The FTC further recommends that companies not maintain SPI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

43. The FTC has brought enforcement actions against businesses for failing to

protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

44. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer SPI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

45. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

46. Best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

47. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

48. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[8]

49. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[9]

50. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual

[8] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs, last accessed May 8, 2024.

[9] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf, last accessed May 8, 2024.

must show evidence of actual, ongoing fraud activity to obtain a new number.

51. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[10]

52. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[11]

53. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiff and members of the Class stolen in

[10] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft, last accessed May 8, 2024.

[11] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf, last accessed May 8, 2024.

the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and the Class. Stolen personal data of Plaintiff and members of the Class represents essentially one-stop shopping for identity thieves.

54. The FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

55. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[12]

56. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. The stolen personal data of Plaintiff and members of the Class has a high value on both legitimate and black markets.

---

[12] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29, last accessed May 8, 2024.

57. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

58. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's former and current customers whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

59. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver license number or government-issued identification number, name, and date of birth.

60. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth

more than 10x on the black market."[13]

61. Among other forms of fraud, identity thieves may obtain driver licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

62. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class members has materialized and is present and continuing, and Plaintiff and Class members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; (e) invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII.

63. Plaintiff and Class members are at a heightened risk of identity theft for

[13] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html, last accessed May 8, 2024.

years to come.

64. The unencrypted PII of Plaintiff and Class members will end up for sale on the dark web because that is the modus operandi of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class members. Unauthorized individuals can easily access the PII of Plaintiff and Class members.

65. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

66. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

67. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted

attacks on the victim.

68. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[14]

69. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

70. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

[14] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/tag/fullz/ (last visited Oct. 2, 2023).

71. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class members.

72. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

73. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

74. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual learns that their PII was compromised, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

75. Plaintiff and Class members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach.

76. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good

name and credit record."[15]

77. These efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[16]

78. And for those Class members who experience actual identity theft and fraud, the GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[17]

79. PII is a valuable property right.[18] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts that include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

80. An active and robust legitimate marketplace for PII exists. In 2019, the data

---

[15] *See* GAO Report *supra* n.35.

[16] *See* Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps, last accessed May 8, 2024.

[17] GAO Report *supra* n.35.

[18] *See, e.g.*, Randall T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

brokering industry was worth roughly $200 billion.[19]

81. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[20]

82. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[21]

83. Conversely, sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[22]

84. As a result of the Data Breach, Plaintiff's and Class members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the PII has been lost, thereby causing additional loss of value.

85. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class members, and of the

[19] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LOS ANGELES TIMES, available at: https://www.latimes.com/business/story/2019-11-05/column-data-brokers, last accessed May 8, 2024.
[20] *See*, e.g., https://datacoup.com/;
[21] Nielsen Computer & Mobile Panel, Frequently Asked Questions, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html, last accessed May 8, 2024.
[22] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/, last accessed May 8, 2024.

foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class members as a result of a breach.

86. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to, upon information and belief, millions of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

87. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class members.

88. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes ——e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

89. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

90. Consequently, Plaintiff and Class members are at a present and continuous risk of fraud and identity theft for many years into the future.

91. The retail cost of credit monitoring and identity theft monitoring can be around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost that Plaintiff and Class members would not need to bear but for Defendant's failure to safeguard their PII.

92. Furthermore, Defendant's poor data security deprived Plaintiff and Class members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for products and/or services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the product and/or service and necessary data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

FACT SPECIFIC TO PLAINTIFF

93. On or about April 1, 2024, Plaintiff was notified via letter from Defendant that he had been the victim of the Data Breach.

94. Plaintiff, at one time, applied for pre-approval of a mortgage that would have been serviced by Defendant, but did not actually end up formally applying for, much less receiving a mortgage serviced by, Defendant.

95. There can be no legitimate business reason for Defendant continuing to maintain Plaintiff's PII, including his Social Security number, for years past his pre-approval application.

96. Plaintiff had no means or ability to stop Defendant from obtaining or deleting his PII.

97. Plaintiff has spent approximately 20 hours dealing with the fallout of the Data Breach, including checking accounts and monitoring his credit.

98. Additionally, Plaintiff is aware of no other source from which the theft of his SPI could have come. He regularly takes steps to safeguard his own SPI in her own control.

V. CLASS ALLEGATIONS

99. Plaintiff brings this action individually and on behalf of all others similarly situated pursuant to rules 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

100. Specifically, Plaintiff proposes the following class definition, subject to amendment as appropriate:

> All individuals in the United States whose PII was disclosed in the Data Breach (the "Class").

101. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

102. Plaintiff reserves the right to modify or amend the definition of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

103. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

104. Numerosity. The Class members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes that the proposed Class includes approximately 211,650 individuals[23] who have been damaged by Defendant's conduct as alleged herein.

105. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA;

c. When Defendant learned of the Data Breach;

d. Whether Defendant's response to the Data Breach was adequate;

e. Whether Defendant unlawfully shared, lost, or disclosed Plaintiff's and Class members' PII;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII

[23] https://apps.web.maine.gov/online/aeviewer/ME/40/bfabbdc9-6593-4e0f-a9b5-bf21a94b2329.shtml, last accessed May 8, 2024.

compromised in the Data Breach;

g. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Defendant owed a duty to Class members to safeguard their PII;

j. Whether Defendant breached its duty to Class members to safeguard their PII;

k. Whether hackers obtained Class members' PII via the Data Breach;

l. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class members;

m. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

n. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class members suffered as a result of Defendant's misconduct;

p. Whether Defendant's conduct was negligent;

q. Whether Defendant was unjustly enriched;

r. Whether Plaintiff and Class members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class members are entitled to additional credit or

identity monitoring and monetary relief; and

t. Whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

106. Typicality. Plaintiff's claims are typical of those of other Class members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class members because, *inter alia*, all Class members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class members arise from the same operative facts and are based on the same legal theories.

107. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

108. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class members in that all of Plaintiff's and Class members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

109. Superiority. A Class action is superior to other available methods for the fair

and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

110. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

111. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class members affected by the Data Breach.

FIRST CLAIM FOR RELIEF
Negligence and Negligence *Per Se*
(By Plaintiff Individually and on Behalf of the Class)

112. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 111.

113. Defendant requires its consumers, including Plaintiff and Class members, to

submit non-public PII in the ordinary course of providing its services.

114. Defendant gathered and stored the PII of Plaintiff and Class members as part of its business of soliciting its services to its consumers, which solicitations and services affect commerce.

115. Plaintiff and Class members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

116. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class members could and would suffer if the PII were wrongfully disclosed.

117. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

118. Defendant had a duty to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

119. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

120. Defendant's duty of care to use reasonable security measures arose as a

result of the special relationship that existed between Defendant and Plaintiff and Class members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of being consumers of Defendant.

121. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

122. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

123. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former consumers' PII it was no longer required to retain pursuant to regulations.

124. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

125. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

126. Defendant breached its duties, pursuant to the FTCA and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class members' PII;

d. Failing to detect in a timely manner that Class members' PII had been compromised;

e. Failing to remove former consumers' PII it was no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

127. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class. Plaintiff and Class members were within the class of persons the FTCA was intended to protect and the type of harm that resulted from the Data Breach was the type of harm it was intended to guard against. 155.

128. Defendant's violation of Section 5 of the FTCA constitutes negligence per se.

129. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and

deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

130. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

131. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' PII would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the entertainment industry.

132. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

133. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

134. It was therefore foreseeable that the failure to adequately safeguard Class members' PII would result in one or more types of injuries to Class members.

135. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

136. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

137. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

138. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

139. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

140. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

141. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach;

(v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

142. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

143. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

144. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

145. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class members in an unsafe and insecure manner.

146. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii)

continue to provide adequate credit monitoring to all Class members.

SECOND CLAIM FOR RELIEF
Breach of Third-Party Beneficiary Contract
(By Plaintiff Individually and on Behalf of the Class)

147. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 111.

148. Upon information and belief, Defendant entered into contracts with its corporate customers to provide services to them; services that included data security practices, procedures, and protocols sufficient to safeguard the SPI that was entrusted to it.

149. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their SPI that Defendant agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the SPI belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

150. Defendant knew or should have known that if it were to breach these contracts with its customers, Plaintiff and Class Members would be harmed.

151. When Plaintiffs and Class Members provided their SPI to Defendant's customers in exchange for Defendant's customer's services, they entered into implied contracts with Defendant under which—and by mutual assent of the parties—Defendant agreed to take reasonable steps to protect their SPI.

152. Defendant breached its contracts with corporate customers by, among other things, failing to adequately secure Plaintiff and Class Members' SPI, and, as a result, Plaintiff and Class Members were harmed by Defendants' failure to secure their SPI.

153. As a direct and proximate result of Defendants' breach, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained incidental and consequential damages including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their SPI; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their SPI, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' SPI. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD CLAIM FOR RELIEF
Unjust Enrichment, In the Alternative
(By Plaintiff Individually and on Behalf of the Class)

154. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 111.

155. This count is pleaded in the alternative to the Breach of Third-Party Beneficiary Contract claim above.

156. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they paid for services from Defendant and in so doing also provided Defendant with their PII. In exchange, Plaintiff and Class members should have received from Defendant the services that were the subject of the transaction and should have had their PII protected with adequate data security.

157. Defendant knew that Plaintiff and Class members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class members' PII for business purposes.

158. Defendant failed to secure Plaintiff's and Class members' PII and, therefore, did not fully compensate Plaintiff or Class members for the value that their PII provided.

159. Defendant acquired the PII through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

160. If Plaintiff and Class members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendant or obtained loyalty program membership at Defendant.

161. Plaintiff and Class members have no adequate remedy at law.

162. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred upon it.

163. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

164. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class members may seek restitution or compensation.

165. Plaintiff and Class members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and Plaintiff's

counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the and integrity of the PII of Plaintiff and Class members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling

personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs

sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, statutory, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

DATED: May 15, 2024

Respectfully Submitted,

/s/ Cristina Perez Hesano
Cristina Perez Hesano (#027023)
PEREZ LAW GROUP, PLLC
7508 N. 59th Avenue
Glendale, AZ 85301
cperez@perezlawgroup.com
Local Counsel for Plaintiff and the Putative Class

Carl V. Malmstrom
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com

Attorney for Plaintiff and the Putative Class